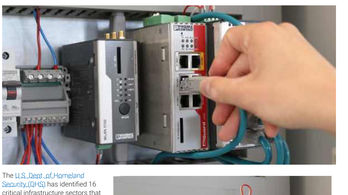
Ensuring SCADA/HMI cybersecurity

Critical industries, such as chemical, energy, transportation, and water/wastewater depend on supervisory control and data acquisition (SCADA) systems for daily operations. Strengthening weaknesses in these systems must be a priority and is a shared responsibility.

BY MARIAM COLADONATO, PHOENIX CONTACT USA NOVEMBER 26, 2016



The U.S. Dept. of Homeland Security (DHS) has identified 16 critical infrastructure sectors that are "so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." These include the chemical, critical manufacturing, energy, nuclear, transportation systems, and water/wastewater sectors.

According to a DHS report from the National Cyber Security and Communications Integration Center and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the ICS-CERT team responded to 295 cyber incidents in U.S. fiscal year 2015, a 20% increase over the previous fiscal year. This included 95 incidents within critical manufacturing, 46 within the energy sector, and 25 within the water and wastewater systems sector.

These industries rely heavily on supervisory control and data acquisition (SCADA) networks for day-to-day operations. If national security is only as strong as its weakest link, the SCADA networks in our critical infrastructure might be that weak point. Strengthening the weaknesses in these systems must be a priority and is a shared responsibility.

The U.S. government has issued several guidelines and recommendations to help secure these critical industries, but most are vague and unenforceable. More than 85% of U.S. critical infrastructure is privately owned or operated, so it is largely up to the infrastructure operators to prepare action plans of prevention, mitigation, incident management, and response.

Why industrial networks are so vulnerable

Many of these SCADA systems have been running for decades. This legacy equipment was designed for the needs of the operational technology (OT) department, rather than the information technology (IT) department. IT and OT traditionally have had different priorities when it comes to security. IT is tasked with protecting a company's data, so confidentiality is the main concern. The OT world was designed for ease of use, data availability and integrity, and uptime, but not necessarily for security.

When programmable logic controllers (PLCs) were introduced to the market decades ago, they solved a specific set of problems: easy maintenance in the field, high uptime, and a life span of 20 to 30 years. In the past, this was fine, because PLCs in the field were typically air-gapped, or isolated from other zones. However, in today's connected world, this isolation is no longer the case. Even an air-gapped, stand-alone system is vulnerable to infection from a universal serial bus (USB) device.

Industrial protocols also present risks because they were not designed with security in mind. Because many of these protocols have been in use for decades, it would be a daunting task to add security at this point. It would require coordinating updates with hundreds of vendors who manufacture products for those protocols and ensuring interoperability of the devices installed around the world.

The growing use of industrial PCs (IPCs) and other human-machine interfaces (HMIs) leads to more vulnerability. While the IPC is built to withstand industrial conditions, it still might be running a commercial version of Windows, so it is susceptible to all of the vulnerabilities that come with that operating system. At least one out of three devices is still running Windows XP, which Microsoft no longer supports. Running antivirus software is difficult and expensive to maintain in an industrial environment, so if a virus infects an IPC, it could affect an entire system.

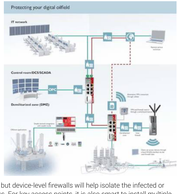
Where to turn for cybersecurity guidance

Both the public and private sectors understand how important it is to increase the security of these systems. In February 2013, the White House established a Commission on Enhancing National Cybersecurity with the goal of strengthening cybersecurity in both the public and private sectors. In addition, many industries have formed cyber security awareness groups to share experiences about the importance of cybersecurity, develop recommended practices, and create guidelines to show asset owners how and where to start taking responsibility for security in their networks.Examples include:

- The North American Electric Reliability Corporation (NERC), a not-for-profit international regulatory authority whose mission is to assure the reliability of the bulk power system in North America, created and regularly update a series of Critical Infrastructure Protection (CIP) standards. It is important to note that 11 of the NERC guidelines are subject to enforcement, making this the only regulated cybersecurity standard today.
- The International Society of Automation (ISA) together with the International Electrotechnical Commission (IEC) developed the ISA99/IEC62443 standard for manufacturing and control systems cybersecurity.
- The American Public Transportation Association (APTA) is currently working on Part 3 in its Recommended Practice for Securing Control and Communications Systems in Transit Environments.
- The Chemical Facility Anti-Terrorism Standards (CFATS) under DHS is dedicated to chemical infrastructure cybersecurity.

These guidelines rely heavily on Recommended Practice: Improving Industrial Control Systems Cyber Security with Defense-in-Depth Strategies, a report from DHS, originally released in October 2009 and updated in September 2016.

Steps to take to protect SCADA and HMI



A defense-in-depth methodology recommends taking a layered approach to cybersecurity. If there is only a single layer of defense, an intruder who knows how to get around that level can easily breach the entire system. For example, if the only level of defense is antivirus software, a new piece of malware that has not been detected can slip through the cracks because the software does not recognize it. Adding multiple layers of defense to a control system will minimize the risk of a serious incident.

Consider the following best practices for adding defensive layers to a control system:

Firewall management: Firewalls should be deployed throughout the control system network, including device-level firewalls at the remote terminal unit (RTU)/PLC/distributed control system (DCS) level (see Figure 1). The potential downsides of this practice are added latency and capital costs, but device-level firewalls will help isolate the infected or disrupted system if an attacker is able to gain access. For key access points, it is also smart to install multiple firewalls from different manufacturers. If an attacker manages to break through one firewall, there still is an additional layer of protection and additional time to patch vulnerabilities.

There are several different types of firewalls, and each has its pros and cons.

- Packet filtering firewalls check the address information in each packet of data against a set of criteria before forwarding the packet. While they have low latency and cost the least, they also offer the lowest level of security.
- Stateful inspection firewalls track active sessions and use that information to determine if packets should be forwarded or blocked. Even with the added security, stateful firewalls are still available at a cost-effective price point and do not add significant latency to the network.
- Deep-packet inspection (DPI) firewalls examine each packet at the application layer and provide the highest level of security. They add latency and are difficult to configure and maintain, so they should be used only in strategic points within an industrial network. They are more common in IT networks, where latency is not as much of a concern.

Security information and event monitoring (SIEM) technologies: SIEM technologies streamline the review of logs, simple network management protocol (SNMP) traps, and event management. SIEM technologies provide a central console for security personnel to review logs from intrusion detection systems, firewalls, and other cybersecurity devices. This can help users comply with monitoring, logging, and review requirements.

Demilitarized zones (DMZs): A DMZ is a protected subnetwork between two other networks (see Figure 2). It can be set up between an untrusted network (e.g., the office network) and a trusted network (the control network). There are several ways to create a DMZ network, but the purpose is to make data from the trusted network available to those who need it and who don't necessarily need direct access to the network.

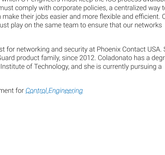
Patch management: As mentioned earlier, security patch management is difficult within legacy industrial control systems, but performing it can fix bugs and close vulnerabilities. Test these patches on a regular basis—at least once a year but more often in some cases—in a controlled environment, before applying the updates to all individual devices. After patches are tested, verify those results with the appropriate vendors.

Authentication and authorization: Authentication is a verification process to ensure that only those people, devices, systems, or other entities with the proper credentials can access the network. It is often used along with authorization, which specifies who has rights to access data. Technologies and practices to enable authentication and authorization include:

- Role-based access control
- Challenge/response authentication
- Physical token/smart-card authorization
- Biometric authentication.

Malicious code prevention: There are several ways to detect, deter, and mitigate malicious code from infecting a network:

- Antivirus software can be a valuable tool that can detect many viruses, but at the rate malware is being introduced, it is difficult to keep up-to-date, especially in an industrial setting. Another downside is that every file must have a unique license per operating system, so the costs can add up quickly.
- Common internet file system (CIFS) integrity monitoring supplements antivirus programs in Windows-based systems and can detect malware on day zero. CIFS integrity monitoring examines file systems to take a baseline snapshot of what the system looks like when it's clean. Most OT devices are static and have little change. CIFS integrity monitoring goes back on a regular basis to monitor whether anything has been modified. If it detects a change, it notifies the appropriate user. It also prevents installation of third-party software (see Figure 3).
- Whitelisting allows the administrator to ensure that only trusted applications can run on the system. To work properly, it requires some administration, but it can prevent malicious files from running.



Virtual LANs: Another technology that can be deployed in networks is virtual LANs, or VLANs. VLANs physically divide networks into smaller, more logical networks to help increase performance and simplify management of the network. A VLAN is actually a network management tool and not designed to detect network security or vulnerabilities. A properly designed VLAN can help mitigate broadcast storms that may occur from hardware failures or cyber incidents.

Data diodes: Data diodes are another access control technology that can be deployed in control system networks. For traffic that needs to be only unidirectional (e.g., operational data being sent to a backup location), a data diode can ensure that no return traffic is allowed back into the protected system. A data diode is a system in which a pair of devices works together; one device has only a physical transmitter while the other has only a physical receiver. Software within the system handles the generation of transmission control protocol (TCP) acknowledgments that are required for many communication protocols.

Encryption technologies: The ISA 99 standard recommends the use of virtual private networks (VPNs) to secure remote connectivity. A VPN allows private networks to communicate over a public infrastructure. It encrypts data across untrusted networks and authenticates access into trusted networks.

Common-sense best practices: Technology is critical in securing control systems but doesn't overlook the human level. SCADA and plant managers need to cultivate a security culture, similar to the safety culture that has become more common over the past decade. Managers should look at the logs and audit them regularly. Set a policy that requires strong passwords and teach employees how to create them. Never use the device's default password.

Securing the future

Nearly every day, reports are published that prove how fragile and vulnerable networks are, including SCADA and the operating systems running in ICS. These reports explain new cyber attacks, viruses, vulnerabilities, and even zero days in detail, which can either push the vendor to fix the problem by pushing out security updates or allow attackers to exploit them. ICS cybersecurity is very important, as we count on these systems to bring electricity, clean water, communication, entertainment, and more to our homes.

The implementation of the methods mentioned above, like a multitiered, defense-in-depth approach, addresses the cybersecurity gap in our critical infrastructure, but there is no single entity responsible for the entire process. Other than the energy industry, no other industry regulations are mandatory, therefore the level of protection depends largely on budgetary restrictions in the organization.

An IT administrator's goal is to maintain the highest level of protection possible in his or her network and systems without interfering with everyday business in which OT engineers must keep the ICS process available and running. At the same time, because both groups must comply with corporate policies, a centralized way to monitor security and manage the network and OS can make their jobs easier and more flexible and efficient. OT, IT, company management, government, and others must play on the same team to ensure that our networks stay secure, available, and accurate.

Mariam Coladonato is the product marketing specialist for networking and security at Phoenix Contact USA. She has worked at Phoenix Contact, supporting the FL mGuard product family, since 2012. Coladonato has a degree in electrical engineering from West Virginia University Institute of Technology, and she is currently pursuing a master's degree in cybersecurity.

This article appears in the *Applied Automation* supplement for *Control Engineering* and *Plant Engineering*.

– See other articles from the supplement below.

Related Articles

- *Simplifying drive-based and controller-based automation*
- *Optimize manufacturing value in real time*
- *A new niche for AppliedAutomation*

RECENT CONTENT

TRENDING TOPICS

